TIMOTHY W. GRINSELL (SBN: 308703)
tim@hoppingrinsell.com
MARGARET B. HOPPIN (*pro hac vice forthcoming*)
margot@hoppingrinsell.com
HOPPIN GRINSELL LLP
11 Hanover Sq., Ste. 703
New York, New York 10005
646.475.3550

Attorneys for Plaintiff JustM2J LLC

UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF CALIFORNIA

JUSTM2J LLC,

Plaintiff,

v.

AYDEN BREWER, JON LITZ, JASON ST. GEORGE, JOHN DOE 1, *et al.*,

Defendants.

Case No.

COMPLAINT FOR:

(1) VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT, 18 U.S.C. §§ 1030, *ET SEQ.*
(2) VIOLATION OF THE FEDERAL WIRETAP ACT, 18 U.S.C. §§ 2510, *ET SEQ.*
(3) FRAUD
(4) CONVERSION
(5) UNJUST ENRICHMENT
(6) IMPOSITION OF A CONSTRUCTIVE TRUST AND DISGORGEMENT OF FUNDS
(7) POSSESSION OF STOLEN PROPERTY IN VIOLATION OF CALIFORNIA PENAL CODE § 496

Plaintiff JustM2J LLC ("JustM2J"), by and through its undersigned counsel, as and for its Complaint against Defendants Ayden Brewer, Jon Litz, Jason St. George, John Doe 1, *et al.* ("Defendants"), alleges as follows:

INTRODUCTION

1. This case involves a scheme (the "Bittensor Attack") to steal, launder, and hide tens of millions of dollars in crypto assets by executing a sophisticated series of cyber-attacks against the participants of Bittensor, a decentralized artificial intelligence network and machine learning protocol developed and maintained by non-party Opentensor Foundation ("Opentensor").

2. Defendants are individuals who conspired to execute the Bittensor Attack and then collaborated in its execution in a series of cyber-attacks between May 22 and July 2, 2024, when the ongoing Attack was discovered and halted by Opentensor. In that time, Defendants victimized 32 Bittensor participants by surreptitiously stealing the "keys" needed to access and control each participant's Bittensor "wallet," where participants stored their crypto assets. They then illegally transferred crypto assets collectively worth over $28 million USD from the participants' wallets to themselves and their affiliates through a complex series of transactions intended to conceal their identities and render the stolen assets untraceable.

3. The named Defendants are software developers and engineers with the requisite skill and information to execute the Bittensor Attack, with multiple demonstrable connections to the Attack and to each other. Two (Brewer and St. George) are recent former Opentensor employees; the third (Litz) is their known affiliate and collaborator and a failed applicant for Opentensor employment. On information and belief, the named Defendants conspired and collaborated with at least one additional, yet unidentified, individual defendant to execute the Bittensor Attack.

4. On May 22, 2024, Opentensor released a routine update to the Bittensor software, "version 6.12.2." Virtually simultaneously, Defendants used a proprietary Opentensor password stolen by St. George to upload a nearly identical, but malicious, version 6.12.2 to PyPI, a software distribution platform used by Opentensor. Like the legitimate version, the malicious version was

denominated "version 6.12.2" and was designed in every way to be indistinguishable from the legitimate version. Defendants' malicious "version 6.12.2," and their use of the stolen Opentensor password to upload that version to PyPI, appeared to authenticate the malicious version to Bittensor participants.

5. As a result, Bittensor participants who downloaded version 6.12.2 from PyPI between May 22 and July 2 unwittingly downloaded Defendants' malicious version of that software. Thereafter, when those participants engaged in certain common activities—like registering on the Bittensor network or executing crypto asset transactions—the malicious package secretly intercepted their wallet keys and sent them to a repository created by Defendants for that purpose.

6. Between May 30, 2024 and July 2, 2024, Defendants used these stolen wallet access keys to steal crypto assets from 32 Bittensor participants, including Nakamoto LLC, Plaintiff's ultimate assignor. Defendants stole approximately $13 million USD in crypto assets from Nakamoto alone.

7. On July 2, 2024 alone, Defendants stole crypto assets from 30 Bittensor participants. The unusual activity raised a red flag for Opentensor, which stopped all transactions on the Bittensor network, placed it behind a firewall, activated a pre-determined "safe mode," and launched a thorough investigation.

8. On July 3, Opentensor discovered the malicious version 6.12.2 uploaded to PyPI and immediately removed it.

9. Plaintiff JustM2J is pursuing claims against the perpetrators of the Bittensor Attack as part of an effort to help make victims whole. Plaintiff brings this action as the ultimate assignee of Nakamoto, one of the Attack's victims. JustM2J anticipates amending this Complaint to include claims assigned by additional Bittensor participants victimized in the Bittensor Attack.

PARTIES

10. Plaintiff JustM2J is a Delaware limited liability company with its principal place of business in Florida. By a valid assignment dated January 9, 2025, JustM2J is the assignee of all claims related to the Bittensor Attack that originally belonged to one of its victims (Nakamoto

LLC). JustM2J has cryptographically verified Nakamoto's ownership of the wallet containing the funds stolen on June 1, 2024. The sole member of JustM2J is a natural person who is a resident of Texas. Thus, JustM2J is a citizen of the state of Texas for the purposes of establishing diversity jurisdiction.

11. Defendant Ayden Brewer is an individual who was employed by Opentensor as a Bittensor developer from 2023 to February 29, 2024. On information and belief, Brewer is a resident of this District, and he participated in the Bittensor Attack from this District. Brewer uses the online handle "Rusty," including on the Bittensor network.

12. Defendant Jason St. George is an individual and, on information and belief, a resident of Tully, New York. St. George was employed by Opentensor as a Bittensor developer until about April 12 2024. St. George uses the online handle "Philanthrope," including on the Bittensor network.

13. Defendant Jon Litz is an individual and, on information and belief, a resident of the State of Missouri. Litz unsuccessfully applied for employment at Opentensor in January 2024. He uses the online handle "0xJones," including on the Bittensor network.

14. The John Doe Defendants are one or more unidentified individual defendants who, on information and belief, collaborated and conspired with Defendants Brewer, St. George, and Litz, to execute the Bittensor Attack.

15. Defendants have maintained, and continue to maintain, multiple private cryptocurrency wallets and cryptocurrency exchange accounts in which they hold digital assets stolen from Bittensor participants, including assets stolen from Plaintiff's assignor Nakamoto. Defendants recently transferred digital assets from the attack worth $300,000 USD on January 20, 2025.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332 because the amount in controversy exceeds $75,000 and, on information and belief, it is an action between citizens of a state and citizens of a foreign state.

17. This Court also has subject matter jurisdiction over this action pursuant to 28

U.S.C. § 1331 because this case involves federal questions under the Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030(a), *et seq*. and the federal Wiretap Act, 18 U.S.C. §§ 2510, *et seq*.

18. This Court has personal jurisdiction over Defendant Brewer because he is a resident of this District.

19. This Court has personal jurisdiction over all Defendants because, on information and belief, they illegally executed the Bittensor Attack from this District.

20. Venue is proper pursuant to 28 U.S.C. § 1391(b)(2) because a "substantial part of the events or omissions giving rise to" Plaintiff's claims in this action occurred in this District, including all acts taken in furtherance of the Bittensor Attack by Defendant Brewer.

FACTUAL BACKGROUND

21. Bittensor is a decentralized network that is designed to foster collaboration and competition among AI researchers and developers and thus to accelerate the development of advanced AI technologies. Bittensor participants can earn rewards in the network's native digital token, TAO, by providing valuable computations or high-quality machine learning models relative to a specific task. It comprises multiple "subnets," each of which is devoted to a specific AI challenge, like image or text recognition. Bittensor is an open-source project, meaning that its source code is made freely available to the public subject to the terms of the MIT open-source license.

22. Nakamoto, Plaintiff's ultimate assignor, is a blockchain technology company whose primary business activity during the relevant period was to earn TAO by performing complex computations related to artificial intelligence challenges.

23. Currently, there are about 8 million TAO in circulation. The market value of a single TAO is about $465 USD, bringing the market capitalization (current circulation times price) to over $3 billion USD.

24. To participate in the Bittensor network, participants need certain software. One such piece of software is a "wallet," which enables participants to receive, store, and transfer TAO. A participant needs a "private key"—a long string of numbers and letters that functions much like a password—to transact with their Bittensor wallet and to send TAO from the wallet.

Private keys thus confer control over the assets in a Bittensor participant's wallet and are therefore carefully protected.

25. The Bittensor network is maintained, developed, and improved by a team of developers and engineers employed by Opentensor. The Opentensor team periodically updates Bittensor software and publishes those updates on distribution platforms for download by Bittensor participants.

26. Defendant Brewer was a member of that team until February 29, 2024, when he departed suddenly, without notice or explanation. Prior to his departure, Defendant Brewer expressed anger that Opentensor had rejected the January 2024 employment application submitted by Defendant Litz, whom Brewer had recommended.

27. Defendant St. George was also a member of the Opentensor team until April 12, 2024. During his tenure, St. George was responsible for programming projects involving the Python language. He was one of the small number of Opentensor employees who had access to Opentensor's proprietary PyPI key—PyPI is a repository specific to Python-language software—used in the Bittensor Attack.

A. Defendants mimic a legitimate Bittensor update.

28. On information and belief, Defendants Brewer, St. George, and Litz entered into an agreement to plan, prepare, and execute the Bittensor Attack, and to hide its profits, in or around April 2024. Pursuant to that agreement, Defendant St. George wrongfully retained Opentensor's proprietary PyPI key upon the termination of his employment. In addition, Defendants developed malicious code intentionally designed to mimic Bittensor code.

29. On information and belief, on May 20, 2024—two days before the scheduled release of a routine upgrade to Bittensor's wallet software—Defendants registered a domain, opentensor.io, intended to appear as belonging to Opentensor. Later, when Bittensor participants who downloaded the malicious version of 6.12.2 executed certain transactions on the Bittensor network, the malicious code would secretly intercept their wallet keys and send them to opentensor.io.

30. On May 22, 2024, Opentensor released a routine upgrade to Bittensor's software, denominated version 6.12.2. The code for version 6.12.2 was (and is) publicly available on Bittensor's open-source code repository, Github. Prior to its release, the status of the update's progress was publicly visible in real time to those observing transactions on the Bittensor blockchain, including Defendants.

31. In the brief interval between the publication of the legitimate version 6.12.2 on Github and its intended publication on PyPI, Defendants uploaded a malicious version of 6.12.2 to PyPI, using Opentensor's stolen proprietary PyPI key. Defendants' malicious version intentionally mimicked the code and filenames of the legitimate version and appeared indistinguishable from the legitimate update. Further, because Defendants used the proprietary Opentensor key to upload their malicious version 6.12.2, and because the PyPI repository is configured to reject duplicative software "versions," Defendants' malicious upload in effect blocked Opentensor's upload of the legitimate version.

32. Bittensor users who downloaded version 6.12.2 from platforms other than PyPI obtained the legitimate version of 6.12.2, and their private wallet keys remained safe.

33. However, Bittensor participants who downloaded version 6.12.2 from PyPI (prior to July 2, 2024) in fact received the malicious version deployed by Defendants. The malicious version appeared to execute the same functions as the legitimate version, but it also covertly intercepted the private key associated with each participant's wallet and then sent those keys to opentensor.io, the domain Defendants had registered on May 20.

B. Defendants steal approximately $28 million in TAO from Bittensor participants.

34. Between May 22, when Defendants uploaded their malicious version of 6.12.2 to PyPI, and July 2, when Opentensor detected suspicious activities on the Bittensor network, Defendants stole approximately $28 million in TAO from 32 Bittensor participants. Defendants stole this TAO from those participants' wallets by using the private keys covertly intercepted by their malicious version of 6.12.2 and transmitted to Defendants at the opentensor.io domain.

35. On May 30, Defendants used one such illegally obtained private key to steal

1,030.9 TAO (about $480,000 USD) from a single Bittensor participant's wallet.

36. On June 1, Defendants used another illegally obtained private key to steal 28,368 TAO (about $13 million) from the Bittensor wallet belonging to Nakamoto, Plaintiff's assignor.

37. On July 2, Defendants transferred 32,395 TAO (about $15 million) from 30 unique Bittensor participant wallets.

38. Immediately after the July 2 attack, Opentensor detected an abnormality in transfer volume and placed the Bittensor network in "safe mode," halting transfers to or from the Bittensor blockchain until it could complete its investigation.

39. On July 3, Opentensor discovered the malicious version of 6.12.2 that Defendants had uploaded to PyPI. This version was immediately removed from PyPI.

40. In addition, Opentensor retained a forensic investigator, contacted law enforcement, and contacted at least one service—the "TAO-wTOA bridge," discussed below—to request a freeze of certain stolen assets in the process of transmission.

C. Defendants launder the stolen TAO following the attacks.

41. After each cyber-attack, Defendants executed a complicated series of additional transactions intended to cover their tracks and hide the TAO they stole from Bittensor participants. As alleged in greater detail below, Defendants exchanged stolen TAO for other crypto assets; sent stolen assets to a cryptocurrency "mixer," a tool to jumble cryptocurrency transactions and obscure their sources; sent stolen assets to an address associated with laundering activities; transferred assets across different blockchains; and distributed stolen assets across a large number of crypto exchanges, including several with no "know your customer" practices ("Non-KYC Exchanges").

42. Nonetheless, Plaintiff's investigators were able to partially trace the stolen TAO and to identify multiple blockchain addresses and cryptocurrency exchange accounts that received the stolen TAO ("Destination Addresses").

i. *The May 30 Attack*

43. The stolen assets—1,030.9 TAO, valued at about $480,000 USD—were first

routed to the "TAO-wTAO bridge," a mechanism that allows the user to convert TAO to wTAO, which (unlike TAO) can be transferred to the Ethereum blockchain.

44. The wTAO was then exchanged for ETH (Ethereum) on Uniswap, a decentralized crypto exchange, and repeatedly transferred.

45. The Destination Addresses for assets stolen in the May 30 attack are: 103 ETH ($412,206 USD) deposited to WhiteBit, a cryptocurrency exchange based in Lithuania; and 0.884 ETH ($3,537 USD) transferred to an Ethereum wallet address which also temporarily received assets stolen in the June 1 attack, described below.

46. The Destination Addresses for the traced endpoints of the May 30 cyber-attack are:

Cryptocurrency and Volume	USD Value[1]	Address Type	Address
103 ETH	$412,206	WhiteBit Deposit Address	0x5e92aB69eB102cFC4A7C507D8Dc3cC1eEdE25Eb0
0.884 ETH	$3,537	June 1, 2024 Hack Address	0x09F76d4FC3bcE5bF28543F45c4CeE9999E0a0AAf

ii. *The June 1 Attack*

47. The stolen assets—28,368 TAO, valued at about $13 million USD—were first routed to the TAO-wTAO bridge, and then temporarily deposited to the same Ethereum wallet address identified above as the traced endpoint for 0.844 ETH of the proceeds of the May 30 attack.

48. The wTAO was then exchanged for ETH, wETH, and USDC[2], using Uniswap. Those assets were, in turn, exchanged further and then repeatedly transferred.

49. They were dispersed across multiple endpoints, including: 987,938 USDC ($987,938 USD) to deposit addresses on Binance, a major global cryptocurrency exchange; 384,192 USDC ($384,192 USD) and 427.9977 ETH ($1,712,846 USD) to deposit addresses on WhiteBit; 351.9987 ETH ($1,408,698 USD) to deposit addresses on HTX, a large cryptocurrency

[1] Calculated using the peak ETH/USD conversion rate over the past 30 days. This same method is used in all the tables that follow.

[2] USDC (USD Coin) is a popular stablecoin cryptocurrency designed to maintain a 1:1 peg with the US dollar.

exchange based in Seychelles.

50. In addition, 10 ETH ($40,020 USD) was forwarded to an Ethereum address known from other unrelated hacks to be associated with money laundering services (the "Link Address") and 300,000 USDC ($300,000 USD) was sent to two private wallet addresses. On January 20, 2025, the private wallet funds were transferred to Coinbase deposit address 0xd5960CA93A0b3fEE31a6B691BCA27e5C36701B83.

51. Significant sums were routed through the Railgun Privacy Protocol, a system designed to obfuscate crypto transaction details. Nonetheless, investigators were able to partially trace 1,205 ETH ($4,822,410 USD) from the Railgun Privacy Protocol.

52. 1,055 ETH ($4,222,110 USD) were sent from the Railgun Privacy Protocol to the Synapse Protocol bridge, a tool for transferring crypto assets between different blockchains, and through multiple transactions thereafter. Of those, 507 ETH ($2,029,014) were ultimately sent to deposit addresses on WhiteBit, Binance, KuCoin, a cryptocurrency exchange based in Seychelles, and MexC, also a cryptocurrency exchange based in the Seychelles.[3] The rest were sent to Non-KYC Exchanges EXCH.CX and Exolix.

53. In addition, 50 ETH ($200,100 USD) were sent from the Railgun Privacy Protocol to a MexC deposit address and 100 ETH ($400,200 USD) were sent to a private wallet address.

54. The Destination Addresses for the traced endpoints of the June 1 cyber-attack are:

Cryptocurrency and Volume	USD Value	Address Type	Address
395,301 USDC	$395,301	Binance Deposit Address	0x8f3100AD91cbfbE8aA58845083B25249f8FfdB29
197,336 USDC	$197,336	Binance Deposit Address	0x9C6D589B7e6Cea55138A3ea1E0AC615126290ED2
99.9999 ETH	$396,198	Binance Deposit Address	0x9C6D589B7e6Cea55138A3ea1E0AC615126290ED2
98.9997 ETH	$396,157	WhiteBit Deposit Address	0x6C030fCf0529baa3FB65532a25aB5154BBE335cB

[3] One of these Binance deposit addresses was also the traced endpoint for assets stolen in the June 1 attack that were *not* routed through the Railgun Privacy Protocol.

384,192 USDC	$384,192	WhiteBit Deposit Address	0x5625f748FF2E0784744a4F974d173924D7219097
63.9997 ETH	$256,087	WhiteBit Deposit Address	0x047050a2A09dc27f23Df519dF7D19074A6a3343f
153.9994 ETH	$616,267	WhiteBit Deposit Address	0x15a8130D8F8AcD4744867b3D51491D1e0189f908
86.9996 ETH	$348,133	WhiteBit Deposit Address	0x65a7437f2F6EF3c203b19af8f1787Db03F1FB20B
24.9995 ETH	$100,009	WhiteBit Deposit Address	0x954f0dF9B7555a755CFd855Bf4809c4e15b732B0
25 ETH	$100,050	WhiteBit Deposit Address	0x6d5f108E94718e346C5eC1C52cE7edd5cDD1a89A
20 ETH	$80,040	WhiteBit Deposit Address	0xe6a2aAE8811c20869a9002A808b7c31a0786588E
28.9 ETH	$115,657	WhiteBit Deposit Address	0xBc9b0B672f8941109Ff37831fa43c922B0935d17
24.9997 ETH	$100,009	HTX Deposit Address	0x56DbE5de6a37f23e85DA00338e1dd58216a40b6c
99.9996 ETH	$396,198	HTX Deposit Address	0x3A9EDb8C26c61F816DeAcE92764964bb1483456E
63.9998 ETH	$256,087	HTX Deposit Address	0x58A6cfc6D9b00E78056f62D8a1efa54741AcEe01
74.9998 ETH	$300,145	HTX Deposit Address	0x01d2B465d5ba513387932290fe1a1644d5A83F22
77.9998 ETH	$312,151	HTX Deposit Address	0x80839E957F5BC7D72e71626636C5FAE202B758e7
99.9996 ETH	$396,198	HTX Deposit Address	0x8C227480B8F9E894a572687799FE5368622FCDC1
85.9997 ETH	$344,167	HTX Deposit Address	0x7824ee032bd857FbbDd9e351F50F5eB80b0ADB13
99.9999 ETH	$396,198	KuCoin Deposit Address	0x6BEe51F3cf378Fc167DFeeF1ea2c856ce6Ec12d8
99.9999 ETH	$396,198	KuCoin Deposit Address	0x3898879e531D2ce92d8FB23cb7aD86d5472060C1
1.999904 ETH	$7,999	KuCoin Deposit Address	0xb3C7E5E8F138F23C461C941AF133BC14F863285E
19.9998 ETH	$80,035	KuCoin Deposit	0x95034c37c1C1D8484089

		Address	Fb46889932402DCA0F82
9.999985 ETH	$40,015	KuCoin Deposit Address	0x85De72B97d6eFe7bFCDaC472fA182F79Da8619DC
9.99987 ETH	$40,015	KuCoin Deposit Address	0x91aC15FE89315867F8BDd7b5bB40D450E2fF0320
4.999909 ETH	$20,005	KuCoin Deposit Address	0x9f02577718bA0505DbB07a13eCc38d809b13399a
50 ETH	$200,100	MexC Deposit Address	0x26658c8e719268e473491E26E5a33e284d1Ea4bF
50 ETH	$200,100	EXCH.CX Deposit Address	0xC49BDbD2F3ed50cD095B108bca6bd7596F2D4ba7
35 ETH	$140,070	EXCH.CX Deposit Address	0xD66766E43cB66628478Ed9D12d076849e81fDfF5
228 ETH	$912,456	EXCH.CX Deposit Address	0x85E14ec0E976414EDE6B38A0b5E5B7879290EF53
100 ETH	$400,200	EXCH.CX Deposit Address	0xCAec170151ABaED4Fc3a158a7c3f78889C0dD9e5
20 ETH	$80,040	EXCH.CX Deposit Address	0xDcDEA8a8cAB06958C590E64937c0D4853744c335
14.9999 ETH	$59,989	EXCH.CX Deposit Address	0x356E2Df6a43A26E340Dae0C3649c26aCcf384082
10.0001 ETH	$40,020	EXCH.CX Deposit Address	0x686Fa4976D8C7EA5BCAc53EB86ea453c44f7c5f3
9.999857 ETH	$40,015	EXCH.CX Deposit Address	0x79Ce9C4160F4AAf5191fC516511c78D0dd24e885
9.999908 ETH	$40,015	EXCH.CX Deposit Address	0x08e637130C4eFBb4e48DC13Cc95c7fC6355A3BdB
4.999893 ETH	$20,005	EXCH.CX Deposit Address	0x34A64406Eb3FBc18994C7B2827E5D266671d011D
4.999963 ETH	$20,005	EXCH.CX Deposit Address	0x22Cb8d3A6D43F86DCBE751e4a2cf235ba1312b79
4.999964 ETH	$20,005	EXCH.CX Deposit Address	0x16929803A0F2392497C81404d7748c65ff9C0c2a
4.999968 ETH	$20,005	EXCH.CX Deposit Address	0x0eC0AC79148305FE817745C18c0aF4Ba07547B98
4.99995 ETH	$20,005	EXCH.CX Deposit	0xF239a90A91e4598b541D

		Address	7D78beaE3621193b9c9D
4.999953 ETH	$20,005	EXCH.CX Deposit Address	0x292685ac52Bdb8fa08aCB50Da3801bd87C4137AF
4.999963 ETH	$20,005	EXCH.CX Deposit Address	0xFF506cD2A2bFDFA80EF62DC22839E16ce40CA4F5
4.999968 ETH	$20,005	EXCH.CX Deposit Address	0xA4F75e61cdAd561bdDD35e921288bd60002f9633
4.999952 ETH	$20,005	EXCH.CX Deposit Address	0x7DA771ec163C461adec09ED2D88f2A5ec62Ff13D
4.99986 ETH	$20,005	EXCH.CX Deposit Address	0xbaE5d5c76c42D93CE65828E9B0c86458Dc5329A7
4.999851 ETH	$20,005	EXCH.CX Deposit Address	0x18c7278D515EF960119148a0c5228718281fC312
9.9999 ETH	$40,015	Exolix Deposit Address	0xfffDEc00c2DD485bFfEdec4eF65489D1F076E1a1
49.999678 ETH	$200,095	Unnamed Service	0x47713cb34FAbd63b39D7C5c6f675dCa39d22762B
1.999818 ETH	$7,999	Unnamed Service	0x47713cb34FAbd63b39D7C5c6f675dCa39d22762B
0.999823 ETH	$3,997	Unnamed Service	0x47713cb34FAbd63b39D7C5c6f675dCa39d22762B
277,906 USDC	$277,906	Railgun.ch Privacy Protocol	0xFA7093CDD9EE6932B4eb2c9e1cde7CE00B1FA4b9
22.41 wETH	$97,688	Railgun.ch Privacy Protocol	0xFA7093CDD9EE6932B4eb2c9e1cde7CE00B1FA4b9
10 ETH	$40,020	Link Address	0x252262813114eB1FF5261E2408B39410a5a8dCCB
300,000 USDC	$300,000	Coinbase Deposit Address	0xd5960CA93A0b3fEE31a6B691BCA27e5C36701B83

iii. *The July 2 Attack*

55. The stolen assets—32,395 TAO valued at about $15 million USD, from 30 unique Bittensor wallets—were initially consolidated in a single Bittensor wallet. From there, 8,295 TAO ($4,587,135 USD) were sent to a KuCoin deposit address and 11,100 TAO ($6,105,000 USD) were sent to a MexC deposit address.

56. 3,000 TAO ($1,395,000 USD) were successfully routed to the TAO-wTAO bridge.[4] The wTAO was exchanged for 224.214 ETH ($897,304 USD) using Uniswap and deposited in an Ethereum wallet address. That same Ethereum wallet address also received six transfers worth a total of 375,768 USDT ($375,768 USD) from KuCoin and MexC that appear to be directly tied to the TAO deposits described above in Paragraph 55. Those 375,768 USDT were then swapped for ETH, combined with the 224.214 ETH obtained from the swapped wTAO, and sent to the Railgun Privacy Protocol, which rendered those assets untraceable.

57. The relevant Destination Addresses for the July 2 hack are:

Cryptocurrency and Volume	USD Value	Address Type	Address
8,295 TAO	$4,587,135	KuCoin	5CrmVKApX6sJybZaL1geHfzvHWeCpbavqrrXgYLCQmhehX2q
11,100 TAO	$6,105,000	MexC	5FqBL928choLPmeFz5UVAvonBD5k7K2mZSXVC9RkFzLxoy2s
333.621 ETH	$1,335,151	Railgun.ch Privacy Protocol	0xFA7093CDD9EE6932B4eb2c9e1cde7CE00B1FA4b9

58. The combined list of Destination Addresses uncovered in Plaintiff's investigation to date appears in the table below.

Address	Entity Label	Cryptocurrency	USD Value
0x70408bb4Dad97c611CAa5A03BB2Bf2B40526FfF0	Binance Deposit 1	99.9999 ETH	$ 348,000
0x9C6D589B7e6Cea55138A3ea1E0AC615126290ED2	Binance Deposit 2	99.9999 ETH	$ 356,000
0x8f3100AD91cbfbE8aA58845083B25249f8FfdB29	Binance Deposit 3	395,301 USDC	$ 395,301
0xd5960CA93A0b3fEE31a6B691BCA27e5C36701B83	Coinbase Deposit 1	300,000 USDC	$ 300,000
0xfffDEc00c2DD485bFfEdec4eF65489D1F076E1a1	Elolix Deposit 1	9.9999 ETH	$ 40,015

[4] Unsuccessful attempts were made to route an additional 10,000 TAO through the TAO-wTAO bridge.

0x356e2df6a43a26e340dae0c3649c26accf384082	eXch Deposit 1	14.9999 ETH	$ 59,989
0x686fa4976d8c7ea5bcac53eb86ea453c44f7c5f3	eXch Deposit 2	10.0001 ETH	$ 40,020
0x08e637130c4efbb4e48dc13cc95c7fc6355a3bdb	eXch Deposit 3	9.999908 ETH	$ 40,015
0x79ce9c4160f4aaf5191fc516511c78d0dd24e885	eXch Deposit 4	9.999857 ETH	$ 40,015
0x0ec0ac79148305fe817745c18c0af4ba07547b98	eXch Deposit 5	4.999968 ETH	$ 20,005
0xa4f75e61cdad561bddd35e921288bd60002f9633	eXch Deposit 6	4.999968 ETH	$ 20,005
0x16929803a0f2392497c81404d7748c65ff9c0c2a	eXch Deposit 7	4.999964 ETH	$ 20,005
0x22cb8d3a6d43f86dcbe751e4a2cf235ba1312b79	eXch Deposit 8	4.999963 ETH	$ 20,005
0xff506cd2a2bfdfa80ef62dc22839e16ce40ca4f5	eXch Deposit 9	4.999963 ETH	$ 20,005
0x292685ac52bdb8fa08acb50da3801bd87c4137af	eXch Deposit 10	4.999953 ETH	$ 20,005
0x7da771ec163c461adec09ed2d88f2a5ec62ff13d	eXch Deposit 11	4.999952 ETH	$ 20,005
0xf239a90a91e4598b541d7d78beae3621193b9c9d	eXch Deposit 12	4.99995 ETH	$ 20,005
0x34a64406eb3fbc18994c7b2827e5d266671d011d	eXch Deposit 13	4.999893 ETH	$ 20,005
0xbae5d5c76c42d93ce65828e9b0c86458dc5329a7	eXch Deposit 14	4.99986 ETH	$ 20,005
0x18c7278d515ef960119148a0c5228718281fc312	eXch Deposit 15	4.999851 ETH	$ 20,005
0x85E14ec0E976414EDE6B38A0b5E5B7879290EF53	eXch Deposit 16	228 ETH	$ 912,456
0xCAec170151ABaED4Fc3a158a7c3f78889C0dD9e5	eXch Deposit 17	100 ETH	$ 400,200
0xC49BDbD2F3ed50cD095B108bca6bd7596F2D4ba7	eXch Deposit 18	50 ETH	$ 200,100
0xD66766E43cB66628478Ed9D12d076849e81fDfF5	eXch Deposit 19	35 ETH	$ 140,070

0xDcDEA8a8cAB06958C590E64937c0D4853744c335	eXch Deposit 20	20 ETH	$ 80,040
0x686fa4976d8c7ea5bcac53eb86ea453c44f7c5f3	eXch Deposit 21	10.0001 ETH	$ 40,020
0x08e637130c4efbb4e48dc13cc95c7fc6355a3bdb	eXch Deposit 22	9.999908 ETH	$ 40,020
0x3A9EDb8C26c61F816DeAcE92764964bb1483456E	HTX Deposit 1	99.9996 ETH	$ 396,198
0x8C227480B8F9E894a572687799FE5368622FCDC1	HTX Deposit 2	99.9996 ETH	$ 396,198
0x56DbE5de6a37f23e85DA00338e1dd58216a40b6c	HTX Deposit 3	24.9997 ETH	$ 100,009
0x01d2B465d5ba513387932290fe1a1644d5A83F22	HTX Deposit 4	74.9998 ETH	$ 300,145
0x58A6cfc6D9b00E78056f62D8a1efa54741AcEe01	HTX Deposit 5	63.9998 ETH	$ 256,087
0x80839E957F5BC7D72e71626636C5FAE202B758e7	HTX Deposit 6	77.9998 ETH	$ 312,151
0x7824ee032bd857FbbDd9e351F50F5eB80b0ADB13	HTX Deposit 7	85.9997 ETH	$ 344,167
0x6BEe51F3cf378Fc167DFeeF1ea2c856ce6Ec12d8	Kucoin Deposit 1	99.9999 ETH	$ 396,198
0x3898879e531D2ce92d8FB23cb7aD86d5472060C1	Kucoin Deposit 2	99.9999 ETH	$ 396,198
0x91aC15FE89315867F8BDd7b5bB40D450E2fF0320	Kucoin Deposit 3	9.99987 ETH	$ 40,015
0x85De72B97d6eFe7bFCDaC472fA182F79Da8619DC	Kucoin Deposit 4	9.999985 ETH	$ 40,015
0x95034c37c1C1D8484089Fb46889932402DCA0F82	Kucoin Deposit 5	19.9998 ETH	$ 80,035
0x26658c8e719268e473491E26E5a33e284d1Ea4bF	MEXC Deposit 1	50 ETH	$ 200,100
0xe8B3A995a1d30e61646401633A1eFa1E4540674d	MEXC Deposit 2	668.642 ETH, 9000 USDC	$ 2,480,000
0x26658c8e719268e473491E26E5a33e284d1Ea4bF	MEXC Deposit 3	50 ETH	$ 200,100
0x5e92aB69eB102cFC4A7C507D8Dc3cC1eEdE25Eb0	Whitebit Deposit 1	103 ETH	$ 412,206

0xBc9b0B672f8941109Ff37831fa43c922B0935d17	Whitebit Deposit 2	28.9 ETH	$ 101,000
0xe6a2aAE8811c20869a9002A808b7c31a0786588E	Whitebit Deposit 3	20 ETH	$ 70,800
0x5F7F71f6f8720f4684107a81be9F57c1a2aB3C2a	Whitebit Deposit 4	9.9997 ETH	$ 35,000
0x047050a2A09dc27f23Df519dF7D19074A6a3343f	Whitebit Deposit 5	63.9997 ETH	$ 241,938
0x65a7437f2F6EF3c203b19af8f1787Db03F1FB20B	Whitebit Deposit 6	86.9996 ETH	$ 331,955
0x15a8130D8F8AcD4744867b3D51491D1e0189f908	Whitebit Deposit 7	153.9994 ETH	$ 585,255
0x6C030fCf0529baa3FB65532a25aB5154BBE335cB	Whitebit Deposit 7	98.9997 ETH	$ 377,414
0x954f0dF9B7555a755CFd855Bf4809c4e15b732B0	Whitebit Deposit 8	24.9995 ETH	$ 94,505
0x5625f748FF2E0784744a4F974d173924D7219097	Whitebit Deposit 9	384,192 USDC	$ 384,373
0x5F7F71f6f8720f4684107a81be9F57c1a2aB3C2a	Whitebit Deposit 10	9.9997 ETH	$ 35,390

D. Defendants' connections to the Bittensor Attack and to each other.

59. The identified Defendants—Brewer ("Rusty"), St. George ("Philanthrope"), and Litz ("0xJones")—have multiple established connections to the Bittensor network, to each other, and to the methods and means used to execute the Bittensor Attack.

60. Brewer and St. George were both deeply involved with the Bittensor network, Bittensor software, and the protocols for Bittensor software updates as recent former Opentensor employees. On information and belief, St. George—who was responsible for Python programming language projects during his tenure at Opentensor and regularly used the proprietary PyPI key to upload Bittensor software updates to PyPI—wrongfully retained that proprietary key upon his departure in order to facilitate Defendants' Bittensor Attack.

61. Prior to his Opentensor employment, Brewer had collaborated with Litz on an NFT (or non-fungible token) project called SKRTT Racing/Hot Wheels and had worked with him at a company called Telynx.

62. Litz unsuccessfully applied to Opentensor for employment in January 2024 and expressly confirmed his use of the "0xJones" handle in connection with his application. Brewer recommended that Litz be hired and then expressed anger when Opentensor rejected Litz's application.

63. During their employment and afterward, Brewer and St. George also created and together owned and operated a Bittensor subnet called "FileTAO." Litz also worked with FileTAO as its primary employee. On information and belief, Brewer and St. George incorporated an entity to serve as the legal owner of FileTAO; negotiated terms of sale and signed a letter of intent to sell FileTAO to an unrelated technology company for millions of dollars; and then, without explanation, suddenly ceased negotiations (and all communications) with the potential purchaser at about the same time as the first attacks. On June 10, Brewer and potentially St. George transferred away a significant amount of FileTAO assets, including to addresses associated with Brewer. On June 11, Brewer and St. George deregistered FileTAO, and FileTAO's Bittensor registration fee was refunded to Brewer.

64. In his work on FileTAO, Litz used the handle "0xJones." Litz was compensated in TAO, and his pattern of exchange transactions resembles the pattern of the attackers in at least two key respects. Specifically, through three specific Ethereum addresses (the "Subnet Wallets"), 0xJones used UniSwap to exchange wTAO for ETH, USDC, and USDT.

65. In addition, blockchain analysis confirms that 0xJones' Subnet Wallets have sent assets to the Link Address, *i.e.*, the Ethereum address associated with money laundering services that was also the final traced endpoint for some of the assets stolen in the June 1 attack.

66. Blockchain data connects a wallet that received funds in the attacks with a wallet owned by 0xJones. After the first two attacks, on June 12, 2024, Ethereum address 0x5E9c2E07027eF258d57D52FeFEf03b835297F5aF ("0x5E")—an address used by 0xJones in the chain of transactions from the Subnet Wallets to the Link Address—bought a series of NFTs from the KillerGF collection on OpenSea, a marketplace for NFTs. The buyer sent the NFTs to a wallet address that also received assets in the June 1 attack, connecting the 0xJones addresses with the June 1 attack.

67. Around the same time, on June 12, 2024, Ethereum address 0xcF0Cad5BE468859BFdF5e6C830C3E7991834b11c ("0xcF") sent funds to the 0x5E address described in the previous paragraph. The 0xcF address received the vast majority of funds that it holds and has held within days of the theft from the same exchanges that received deposits from the attackers. It was also initially funded on February 8, 2024 by an address used to create the SKRTT Racing/Hot Wheels NFT project, connecting Brewer and Litz to this address. Comcast IP address 67.187.194.119—out of Citrus Heights, California—is associated with one of the deposits to the 0xcF address. In addition, on August 26, 2024, the 0xcF address made a purchase through Travala.com, an online travel service offering flights and hotels and which accepts payment in digital assets.

68. Around the time of the attack, 0xJones' social media accounts on X and Telegram were deactivated. 0xJones also deleted his messages on the Bittensor Discord server.

E. Damages

69. By a valid assignment agreement dated January 9, 2025, all right, title, and interest in any and all claims and causes of action Nakamoto had or may have had against the perpetrators of the Bittensor Attack have been assigned to JustM2J.

70. JustM2J has thus been damaged and is entitled to recover from Defendants the 28,368 TAO (or an equivalent value) stolen in the June 1, 2024 cyber-attack, as well as the substantial costs incurred to investigate the Bittensor Attack and to trace the stolen assets.

COUNT 1: Violation of The Computer Fraud and Abuse Act

71. JustM2J incorporates by reference as though fully set forth herein the allegations in the foregoing paragraphs.

72. Defendants violated the Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030(a)(2)(C), 1030(a)(4), and 1030(a)(5)(C), by accessing protected computers without authorization, by doing so knowingly and with an intent to defraud, by furthering fraudulent activity thereby to obtain something of value, and by causing damage or loss.

73. Nakamoto's wallet, the wallets of other Bittensor participants, and Opentensor's

PyPI account are hosted on "protected computers" as defined under 18 U.S.C. § 1030(e)(2)(B) because they are used in interstate or foreign commerce.

74. Defendants intentionally accessed these protected computers without authorization to publish their malicious version 6.12.2 on PyPI, to fraudulently obtain valuable information from Bittensor participants that downloaded that malicious software, including their private +keys, and to fraudulently access Bittensor participants' wallets and steal their crypto assets.

75. By intentionally and without authorization accessing these protected computers, Defendants caused damage or loss to multiple Bittensor participants, including Plaintiff's assignor Nakamoto.

76. JustM2J, in the shoes of its assignor, has suffered losses and damages far in excess of $5,000, plus interest, from and after the time of Defendants' unjust enrichment, and as a direct result of the unauthorized access alleged herein. JustM2J has also incurred over $5,000 in loss in the form of investigation costs following Defendants' attack.

77. JustM2J is empowered to bring this claim under 18 U.S.C. § 1030(g) and is entitled to compensatory damages, injunctive relief, and equitable relief.

COUNT 2: Violation Of the Wiretap Act

78. JustM2J incorporates by reference as though fully set forth herein the allegations in the foregoing paragraphs.

79. The federal Wiretap Act, 18 U.S.C. § 2510, *et seq.*, prohibits intentionally "intercept[ing], endeavor[ing] to intercept, or procur[ing] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication" and intentionally using or disclosing the contents of such illegally intercepted communications. *Id.* § 2511(1).

80. Defendants intentionally designed and published the malicious version 6.12.2 update in order to covertly intercept electronic communications by Bittensor participants that downloaded version 6.12.2 to their respective computers from PyPI, without their consent.

81. Defendants' malicious version 6.12.2 covertly and without authorization intercepted electronic communications transmitted by those Bittensor participants in the course of executing certain transactions on the Bittensor network, and then transmitted their contents—

including the private keys to each participant's Bittensor wallet—to the domain Defendants had registered for that purpose on May 20, 2024.

82. Defendants then used the contents of these illegally intercepted communications, *i.e.*, the private keys, to steal crypto assets from the Bittensor wallets belonging to their victims, including Plaintiff's assignor Nakamoto.

83. Plaintiff is authorized to bring this claim under 18 U.S.C. § 2520 and is entitled to compensatory damages under 18 U.S.C. § 2520(c), punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT 3: Fraud

84. JustM2J incorporates by reference as though fully set forth herein the allegations in the foregoing paragraphs.

85. Starting on May 22, 2024, Defendants intentionally misrepresented their malicious version 6.12.2 as a legitimate update to the Bittensor network published by Opentensor.

86. Defendants knew that their malicious version 6.12.2 was not the legitimate 6.12.2.

87. Defendants intended Opentensor and Bittensor participants, including Nakamoto, to rely on this appearance of legitimacy.

88. In fact, Defendants intended this deception in order to steal digital assets of Bittensor participants.

89. Opentensor and Bittensor participants justifiably relied on this appearance of legitimacy.

90. Bittensor participants were damaged as a result, and Nakamoto has duly and properly assigned its claims for damages to JustM2J. JustM2J is therefore entitled to recover damages in an amount to be proven at trial.

COUNT 4: Conversion

91. JustM2J incorporates by reference as though fully set forth herein the allegations in all of the foregoing paragraphs.

92. Every Bittensor participant victimized in the Bittensor Attack, including Plaintiff's assignor Nakamoto, owns and has exclusive rights to possess the digital assets stored in their

respective Bittensor wallets.

93. Defendants unlawfully obtained access to Opentensor's PyPI key, unlawfully impersonated Opentensor, unlawfully stole Bittensor participants' private keys, and unlawfully took over $28 million in digital assets from those Bittensor participants, including Plaintiff's assignor Nakamoto, over the course of the Bittensor Attack.

94. Defendants unjustly retain control over these assets, depriving Bittensor participants of their digital assets and all associated rights, including their rights to withdraw, convert, transfer, or invest these digital assets.

95. Bittensor participants, including JustM2J in the shoes of its assignor, have suffered resulting damages in an amount to be proven at trial, plus interest from and after the time of conversion, and the costs of investigation of Defendants' attack.

COUNT 5: Unjust Enrichment

96. JustM2J incorporates by reference as though fully set forth herein the allegations in all of the foregoing paragraphs.

97. Defendants unlawfully obtained access to Opentensor's PyPI key, unlawfully impersonated Opentensor, and used this access to steal and receive the benefit of approximately $28 million in digital assets, including Nakamoto's 28,368 TAO.

98. Defendants unjustly retain control over these assets, depriving Bittensor participants of their right to withdraw, convert, transfer, or invest these digital assets.

99. As a result of Defendants' unjust enrichment, JustM2J, in the shoes of its assignor, has suffered damages in an amount to be proven at trial, plus interest from and after the time of unjust enrichment and the costs of investigation of Defendants' attack.

COUNT 6: Imposition of a Constructive Trust and Disgorgement of Funds

100. JustM2J incorporates by reference as though fully set forth herein the allegations in the foregoing paragraphs.

101. As set forth above, Defendants, through actual fraud, misappropriation, and theft, wrongfully obtained Bittensor participants' digital assets, which in equity and good conscience Defendants and their co-conspirators should not be permitted to hold.

102. The digital assets at issue are specific, identifiable property and can be traced to the Destination Addresses and elsewhere.

103. Any and all assets being held by Defendants or their co-conspirators in the Destination Addresses must be held in trust for JustM2J, as the proper assignee of Nakamoto's claims against Defendants, as Defendant is not entitled to the benefit of wrongfully misappropriated and stolen funds.

104. The stolen digital assets identified herein that are being held by Defendants or their accomplices in the destination addresses must be disgorged to JustM2J.

COUNT 7: Violation of California Penal Code § 496

105. JustM2J incorporates by reference as though fully set forth herein the allegations in the foregoing paragraphs.

106. This cause of action asserts a claim against Defendants for the actual theft of Bittensor participants' property as well as for receiving and aiding in concealing the stolen property.

107. In pertinent part, Cal. Penal Code § 496(a) imposes liability upon "[e]very person who buys or receives any property that has been stolen or that has been obtained in any manner constituting theft or extortion, knowing the property to be so stolen or obtained or who conceals, sells, withholds, or aids in concealing, selling, or withholding any property from the owner, knowing the property to be so stolen or obtained" and provides that "[a] principal in the actual theft of the property may be convicted pursuant to this section."

108. Furthermore, Cal. Penal Code § 496(c) provides: "Any person who has been injured by a violation of subdivision (a) or (b) may bring an action for three times the amount of actual damages, if any, sustained by the plaintiff, costs of suit, and reasonable attorney's fees."

109. Plaintiff's assignor Nakamoto and other victims of the Bittensor Attack were damaged by Defendants' theft of digital assets from their respective Bittensor wallets.

110. Defendants knew the property was stolen.

111. Defendants received and had (and still have) possession of the stolen property.

112. Nakamoto's claims against Defendants have been properly assigned to JustM2J.

113. Defendants are liable to JustM2J for three times the amount of Nakamoto's actual damages, the costs of this suit, and all reasonable attorneys' fees.

PRAYER FOR RELIEF

114. NOW, THEREFORE, JustM2J respectfully requests that this Court enter judgment in favor of Plaintiff as follows:

115. For the equitable imposition of a constructive trust over the property taken by Defendants from the Bittensor network and from Bittensor participants between May 22 and July 2, 2024, currently held by or on behalf of Defendants in the Destination Addresses identified herein, and for entry of an Order directing that the wrongfully obtained property belonging to Nakamoto be restored to JustM2J;

116. For equitable restitution, including, without limitation, restoration of the *status quo ante*, and return to Plaintiff all cryptocurrency taken from Plaintiff's assignor in connection with the Bittensor Attack;

117. For compensatory, incidental, and consequential damages, in an amount to be determined, for harms suffered by JustM2J, in the shoes of JustM2J's assignor, by Defendants' unlawful conduct and for enforcement costs to stop Defendants' unlawful conduct;

118. For punitive, exemplary, and any other damages authorized by law, including treble damages under Cal. Penal Code § 496(c);

119. For prejudgment and post-judgment interest on the full amount of damages;

120. For injunctive relief, including an order enjoining Defendants from moving and dispersing the stolen digital assets;

121. For JustM2J's costs incurred in order to investigate the Bittensor Attack and trace the stolen assets;

122. For JustM2J's attorneys' fees according to proof, and costs incurred, to the extent permitted by law; and

123. For such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

124. Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff hereby demands a trial

by jury of all issues triable in this action.

DATED: January 27, 2025

Respectfully Submitted,

HOPPIN GRINSELL LLP

By: */s/ Timothy W. Grinsell*

Timothy W. Grinsell (SBN 308703)
Margaret B. Hoppin (pro hac vice forthcoming)
11 Hanover Sq.
New York, NY 10004
Telephone: 646-475-9550
tim@hoppingrinsell.com
margot@hoppingrinsell.com

Attorneys for Plaintiff